IDA

INSTITUTE FOR DEFENSE ANALYSES

US and Coalition Forces Data (Semantic) Interoperability Study

Dale E. Lichtblau, Project Leader

Richard D. Bleach

May 2010

IDA Document D-4033

Log: H 10-000135

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About this Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract DASW01-04-C-0003,Task BC-5-3045, "US and Coalition Forces Data Interoperability Study," for the ASD(NII)/DoD CIO. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-4033

US and Coalition Forces Data (Semantic) Interoperability Study

Dale E. Lichtblau, Project Leader

Richard D. Bleach

Preface

This document was prepared by the Institute for Defense Analyses (IDA) under Task Order BC-5-3045, "US and Coalition Forces Data Interoperability Study," in support of the Army Studies Program. Its overall purpose is to assess the extent of data (or semantic) interoperability among US and coalition command and control (C2) information technology (IT) systems. There have been three deliverables published previously: (a) Results of Effort to Determine Set of Information Systems to be Analyzed, (b) Definition and Measurement of US and Coalition Force Data Interoperability, and (c) Data Collection Materials and Data Collection Results. This final report consists of a consolidation of the remaining task order deliverables: (d) Annotated Briefing of Analysis Results of Collected Data, (e) Annotated Briefing Identifying Data Interoperability Barriers/Capabilities Gaps, and (f) Final Report Documenting Programmatic Approach to Enhancing Data Interoperability as specified in the amended task order.

The IDA team would like to thank the following individuals for their generous support and cooperation in providing information for this study: Mr. Robert Aaron (Army Test and Evaluation Command); Mr. Mark Blatherwick (Allied Command Transformation (ACT), NATO); CPT Andrew Boggs (USARPAC); LTC Hattie Bouyer (Army CIO/G-6); LtCol Robert Buzby (Marine Corps Tactics and Operations Group (MCTOG)); CDM David Culler (Allied Command Transformation (ACT), NATO); Mr. John Gillette (Tactical Ground Reporting (TIGR) system); Mr. Bruce Haberkamp (Army CIO/G-6); Mr. Robert Hartel (Army TRADOC); Mr. Todd Henry (Combined Information Data Network Exchange (CIDNE)); LTC Sharon Jacobs, (DoD Joint Test & Evaluation Joint Data Exchange); Mr. Robert Landry (Army CIO/G-6); Mr. Kevin Moffat (Combined Information Data Network Exchange (CIDNE)); COL David Moore (Army PM Battle Command); Mr. Peter Morosoff (E-MAPS, Inc.); LtCol Al Ridenhour (USMC Warfighting Lab); Ms. Lisa Roberts (Command Post of the Future (CPOF)); Mr. Lewis Saunders (Army CIO/G-6); Mr. Anthony Sieber (Army CIO/G-6); Mr. Stephen Specht (Army PM Battle Command); LtCOL Mark Wickham (Joint Improvised Explosive Device Defeat Organization (JIEDDO)); Ms. Erin Wolff (Joint Improvised Explosive Device Defeat Organization (JIEDDO)).

The following IDA research staff members were reviewers of this document: Dr. Donald J. Goldstein, LTG Peter A. Kind (USA, ret.), Dr. Peter S. Liou, and Dr. Margaret E. Myers.

Table of Contents

List of Figures

List of Tables

Executive Summary

This study was conducted to objectively examine and quantitatively determine the extent of *semantic interoperability* among command and control (C2) information technology (IT) systems used to support US and coalition forces. The overall objective was to advance warfighter effectiveness and enhance warfighter protection by recommending ways in which semantic interoperability—a necessary condition for the *common understanding of shared information*—might be improved. Specifically, we examined the degree of semantic interoperability among systems used to report and share significant activity (SIGACT) information, particularly with respect to counterinsurgency (COIN) operations and improvised explosive device (IED) data. The latter is critically important in counter-IED (C-IED) operations. By semantic interoperability we mean the capability to convey data or information among warfighters via IT systems in such a way that the warfighters come to have a common, shared understanding of the operational situation.

We concluded that there is a low level of semantic interoperability between major US and coalition C2 IT systems. The capability of these systems to ensure *common understanding of shared information* among our warfighters and coalition partners is poor**.** This assessment is based on a quantitative study of the extent of *semantic interoperability* afforded by five major C2 systems used to report and share SIGACT information. Given the US's current overseas contingency operations (OCOs), these findings expose a significant capability gap: achieving common understanding of shared information among warfighters.

The study was undertaken to answer three questions:

- How should the concept of "data interoperability between ground forces information systems" be rigorously defined and measured?
- What data collection techniques would be most effective and efficient in obtaining the facts necessary for the determination and analysis of data interoperability among ground force information systems?
- What are the main barriers to data interoperability and how might they best be breached?

We defined "semantic interoperability" as the ability of IT systems to *exchange* information such that human users of the systems could come to have a *common understanding* of the information that was exchanged. We devised a *quantitative* measure of the degree of semantic interoperability between different IT systems in terms of the commonality of the terminology used in the systems' respective data models.

We recommend the adoption of both the study's definition of *semantic interoperability* and the metrics we devised to assess the degree of interoperability among US and coalition IT systems.

We recommend that these data collection techniques and the analytical methodology employed be used in subsequent studies that address the semantic interoperability issue.

We used a variety of data collection techniques, including interviews with warfighters; review and hands-on analysis of user manuals, IT system data models, domain lexicons, and actual system user interfaces; review of previous studies and reports; and anecdotal material.

We found several principal barriers to US and coalition forces interoperability:

(1) The use of different and non-harmonized terminology for SIGACT reporting
(2) Rigorously defined lexicons are not developed regularly during the development of doctrine
(3) The lack of standard procedures and formats for reporting the event information that is usually used to generate SIGACT reports
(4) Overly complex mechanisms for the exchange of information between the IT systems
(5) COIN and C-IED tactics, techniques, and procedures (TTPs) have not been fully codified in official doctrine
(6) Official doctrine is not used to fully inform the design, development, and deployment of C2 programs of record (POR)
(7) Training in doctrine and in the IT systems designed to support that doctrine is not conducted concurrently
(8) The IT systems intended to support the warfighter are not being used consistently at all relevant commands

To overcome the main barriers to US and coalition forces interoperability we recommend that the Army

(1) Ensure that deployed (and deploying) IT systems use common data models (or mediation services), thus satisfying one necessary condition for semantic interoperability
(2) Make the development of rigorously defined lexicons—the necessary foundation for unambiguous structure data—a central feature of warfighting doctrine
(3) Develop a concept of operations (CONOPS) and implement TTPs that formalize and standardize event reporting and report formats at all command echelons, particularly at the tactical level
(4) Reduce the complexity of the information exchange process by reducing the number of different systems and communications processes used to effect information sharing
(5) Make the development and publication of official doctrine a priority; accelerate the development of doctrine that directly affects warfighting and that is supported in IT systems

(6) Ensure that IT systems incorporate, mirror, or otherwise fully embody the language of doctrine, at the semantic level using structured data; to this end iterate the development of doctrinal products in such a way as to eventually produce artifacts (e.g., Joint Publications) whose conceptual clarity, precision, and detail in the description of processes and terminology can be used to develop any IT system the doctrine needs to instantiate; close the gap between doctrine writers and the IT system developers so that the latter become the information technology builders of the former
(7) Merge training in doctrine and training in the use of applicable IT systems into a single training package and train warfighters in doctrine and its supporting IT systems concurrently
(8) Ensure that information processing requirements originate from the warfighter and that IT systems are made available to all relevant command echelons; ensure that the automated tools do not create additional burdens on the warfighter

The adoption and implementation of these recommendations will greatly improve the degree of semantic interoperability among US and coalition IT systems and will enhance, in turn, warfighter effectiveness and warfighter protection.

The major interoperability challenge addressed in this study is at the semantic level, or at the application and presentation levels of the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) Reference Model. Technical problems, alluded to in the preceding paragraph, occur at the lower levels of OSI Model. Interoperability of IT systems at the top two levels of the model, at least in the C2 domain, in a way that affords common understanding among the users of those systems, remains to be accomplished. Put another way: we know how to do electronic interconnection technically; we don't, it seems, know how to ensure semantic interoperation very well. We continue, however, to build IT systems that do not support the warfighters' need for shared understanding in a simple and effective way. As a consequence, many IT systems are not used.

Finally, interoperability at the semantic level is a function of several factors. These factors include information understanding which, in turn, is critically dependent upon the semantic alignment of the underlying data models—either directly or via mediation tools; basic data exchange; IT systems that embody current warfighting doctrine; warfighter training in both doctrine and the IT tools being provided for the warfighter's use; the commander's willingness to use the IT tools when they are appropriate; and, finally, the simple ability of the warfighter to acquire and apply the skills needed to take full advantage of the technology.

1. Introduction

1.1 Study Purpose

The purpose of this study was to examine how to improve warfighter effectiveness and protection by analyzing the semantic interoperability of the IT systems provided to the warfighter.[1]

The study objective was to develop a programmatic and effective approach to enhancing semantic interoperability among US forces and their coalition partners by addressing the following questions.

- How should the concept of data interoperability between ground forces IT systems be rigorously defined and measured?
- What data collection techniques would be most effective and efficient in obtaining the facts necessary for the determination and analysis of data interoperability among ground force IT systems?
- What are the main barriers to data interoperability and how might they best be breached?

To answer these questions the study:

- Objectively determined and quantitatively described the extent of semantic interoperability among legacy IT systems provided to the warfighter
- Identified the main reasons for this lack of interoperability
- Recommended specific steps to improve semantic interoperability

1.2 Assumptions

We relied on previous studies and reports,[2] warfighter interviews, and anecdotal remarks to justify the assumption that semantic interoperability—defined generally as the *common*

[1] Reference 1 defines *information system* as the entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. We are using the term *IT system* in a narrower sense to mean the computer hardware and computer software components of an *information system* as defined by Joint Publication 1-02 (Department of Defense Dictionary of Military and Associated Terms). If there is no risk of misinterpretation, we sometimes use the single word *system* when we mean *IT system*.

[2] For example, references 2 and 3.

understanding of shared information—is important for both warfighter effectiveness and protection. The warfighter wants rapid access to easily understandable data.[3]

On the basis of these studies, reports, anecdotes, and interviews, we assumed that the warfighter needs timely information about current activities in an area of operations to develop actionable intelligence, build situational awareness and understanding, and assist with the decision making process. The real-time exchange of this information from the observer back to the command post and its redistribution to higher, adjacent, and subordinate units for analysis and action is assumed to be important to meeting the needs of commanders and their staffs. Our initial assumption was that semantic interoperability can help to achieve a common understanding of this shared information.

1.3 Study Scope

This study was limited to US and coalition C2 systems that are used to share significant activity reports (SIGACTs); specifically: the Combined Information Data Network Exchange (CIDNE), the Command Post of the Future (CPOF), Force XXI Battle Command Brigade and Below (FBCB2), the Tactical Ground Reporting (TIGR) system, and the Joint Operations/Intelligence Information System (JOIIS) were selected for analysis. JOIIS is a system used by the United Kingdom. These systems contain data associated with COIN and C-IED operations, which are important to current Overseas Contingency Operations (OCOs).

Figure 1 illustrates, conceptually, the scope of information that was studied. The rectangle labeled "universe of discourse," denotes the language (or concepts) used, wholly or in part, by each IT system. The two colored rectangles nested within the larger "universe of discourse" signify that COIN- and C-IED-related reports are a subset of SIGACTs. Each of the five circles delineates those portions of the universe of discourse unique to the indicated IT system. The various overlapping or intersecting regions are those subsets of the data models of the respective systems that use the same terms or language.[4] The region of intersection at the center of the diagram denotes the commonality—if any—in the data models of the corresponding systems for COIN and C-IED with respect to SIGACTs.

[3] Reference 3

[4] The diagram is notional and does not reflect the measurement results of this study.

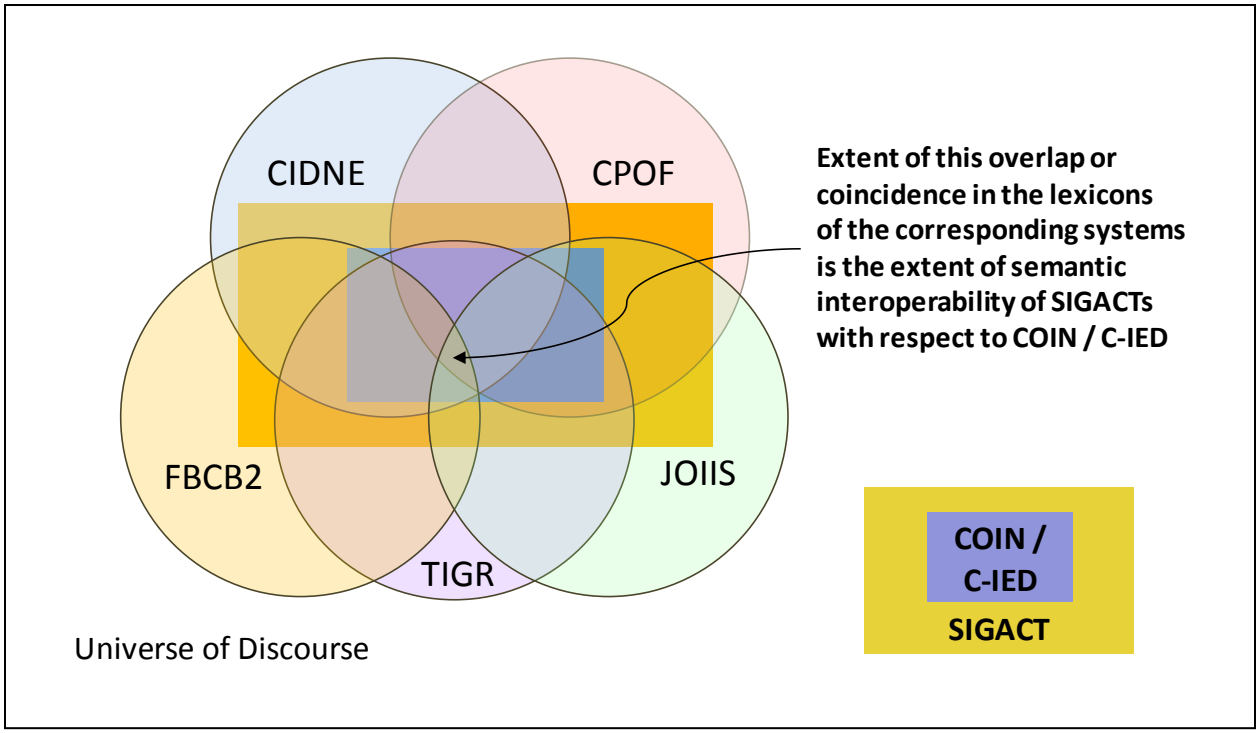

Figure 1. Study Focus

There are several key factors that contribute to and affect semantic interoperability among warfighters: these include doctrine, understanding (including training), exchange, leadership, and ability. These factors can be considered as part of the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) framework.

We did not study traditional impediments to IT systems interoperability associated with inter-computer communications and global networking. These impediments include spectrum and security constraints such as limited bandwidth and multi-level security networks. We believe these impediments are primarily engineering problems and are gradually being overcome.

1.3.1 Doctrine

Ideally, language used by the warfighter should be codified in official *doctrine*. Often it is, but if it is not, there is no authoritative source or policy that can be used for training, command and control, or IT systems development.

1.3.2 Information Understanding

If the language of the warfighter is codified in doctrine, it is important that the warfighter *understand* that language and properly use the common doctrinal *vocabulary*. In other words, the warfighter must be well *trained* both in doctrine and in consistent TTPs. The Service Schools generally bear this training responsibility. Moreover, the warfighter must be trained to use the equipment, services, and procedures that are designed and developed to support the

warfighter and that, ideally, implement doctrine.[5] It is especially important that IT system that are deployed to support the warfighter effectively execute the doctrine. The need to train developers in the doctrine for which they are building IT systems is critically important, but too often overlooked.

1.3.3 Information Exchange

The capability to transfer data among IT systems is necessary to achieve semantic interoperability according to the definition given in this report. Providing this capability in an organized way that avoids complexity supports the warfighter by helping to achieve Department of Defense (DoD) net-centric goals of data accessibility and interoperability.

1.3.4 Leadership

Being well trained is not necessarily sufficient to achieve the basic understanding needed to realize semantic interoperability. Effective leadership is also necessary. Commanders must order and enforce the execution of operations in accordance with relevant doctrine and TTPs (or clearly specify when a departure from doctrine is necessary).

1.3.5 Ability

The simple ability (and will) of the individual warfighter to execute the mission is crucial to the effective semantic sharing of information when using automated information technology. Regardless of the level and quality of doctrine and supporting tools, training, and leadership, the individual warfighter must have the basic ability (and will) to perform as expected.

1.4 Study Methodology

The study was divided into four phases in order to sequentially build on activities that included identifying data, defining and measuring semantic interoperability, collecting and analyzing data, and developing findings and recommendations.

The first phase was focused on refining the scope of the study, identifying the PORs and other systems to be reviewed, and collecting the specific data (data models and information flows) that needed to be analyzed.

In the second phase, we researched interoperability measurement schemes[6] and then developed a semi-formal definition of semantic interoperability that captured our intuitions regarding the concepts of common understanding and data sharing (exchange). We then devised a methodology for measuring (and thus quantifying) the degree of semantic interoperability between two or more distinct IT systems. Two related but distinct notions are central to this interoperability metric: term-level and information-level commonality. This latter concept—information-level commonality—was the metric we then applied to the collected data to obtain preliminary study results.

[5] Reference 18
[6] Reference 5

The data collection methods and analytical methodology were documented in phase three.

The final phase of the study produced a compilation of an account of the overall study plan, the final results of the study, recommendations, initiatives precipitated from preliminary results, and suggestions for further research and work. That material is contained in this final report. Figure 2 depicts the study methodology.

We believe that the methodology devised during this study is not limited to assessing semantic interoperability in the COIN and C-IED sub-domains of the broader C2 domain. It should be applicable for assessing the semantic interoperability between IT systems for any DoD mission area, whether warfighter, business, or intelligence.

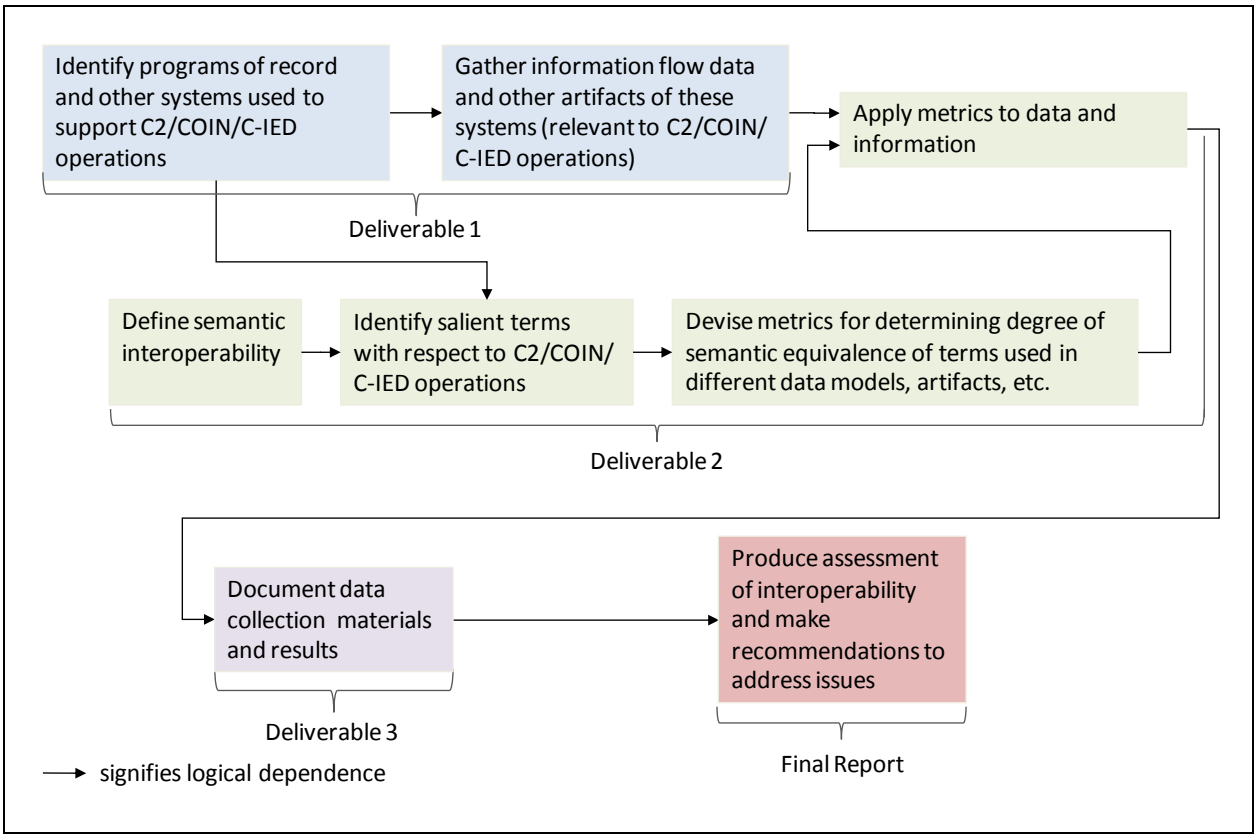

Figure 2. Study Methodology

2. Analysis of Data Interoperability

2.1 Semantic Interoperability Defined

Two or more (distinct) IT systems, $S_1 \ldots S_n$, are defined to be *semantically interoperable* with respect to a domain of discourse, *D*, if and only if any *information* expressible with the vocabulary and syntax of *D*, and processable by $S_1 \ldots S_n$,

- Can be *exchanged* among $S_1 \ldots S_n$, and
- All users of systems S_i and S_j will *understand* any information conveyed from S_i to S_j in exactly the same way.

By *domain of discourse,* we mean a (reasonably) circumscribed subset of the universe of discourse.

By *information,* we mean that which is expressed by any grammatical, declarative, and semantically coherent sentence (i.e., a *statement*).

A person understands what a statement expresses (i.e., understands the information conveyed by the statement) if the individual understands the state of affairs (the fact(s)) denoted and connoted by the sentence. For example, a person understands the term *cat* if a person understands what the term commonly *denotes* (a certain kind of mammal) and what the term commonly *connotes* (a mammal often used in contrast to dog, etc.). A subject, verb, and object of a sentence such as "The cat is on the mat" can be considered as an ordered-triple of terms (e.g., <"the cat", "is", "on the mat">) that conveys common information (fact(s)) for potential semantic interoperability.[7]

Distinctions are often drawn between data, terms, information, and understanding within a domain of discourse.

For the purposes of this study, we define the term *data* ostensively by example: the number 32 is a piece of data when used in the statement "Water freezes at 32 degrees Fahrenheit."

For the purposes of this study, a *term* is a linguistic artifact used with a generally understood common denotation and common connotation among members of a linguistic community. For example, the words *water*, *freezes*, *thirty-two*, *degrees*, and *Fahrenheit* are *terms*.

[7] We are simplifying, of course. The subject of the example sentence is a noun phrase, "the cat." The object is a prepositional phrase, "on the mat." For representation purposes within an information system, the noun phrase becomes an identifier of an individual cat; the verb can be treated as the two-place positional relation, "is on"; and the object , "the mat," is another identifier denoting a particular, individual mat.

For the purposes of this study, *information* is expressed by any statement composed of the terms (of a universe of discourse) in accordance with the syntactic and semantic rules of the linguistic community that uses that universe of discourse. For example, the statement "Water freezes at 32 degrees Fahrenheit" conveys (expresses) *information (a fact)*. The statement "Water boils at 100 degrees Fahrenheit" conveys (expresses) *false information (contrary to a fact)*. Noam Chomsky's famous nonsense sentence, "Colorless green ideas sleep furiously," is neither true nor false.[8]

For the purposes of this study, *understanding* is defined as a cognitive state of an individual with respect to both the terms of a domain of discourse and the information expressible with the terms of that domain of discourse. A person understands a term if the individual understands the commonly understood denotation (what the term *refers* to) and the connotation (the meanings) of the term. (The classic example that illustrates this distinction is provided by the terms *morning star* and *evening star*. Both have the same denotation (reference), that is, the planet Venus, but they differ in their connotations.)

The expressions *domain of discourse* and *universe of discourse* are relative to the overall discussion or study, and a domain of discourse is always a subset of the universe of discourse under consideration.

The domain of discourse used in this study is SIGACT reports for COIN of C2 operations of US and coalition forces.

The two key ideas in the definition of semantic interoperability described above can be graphically rendered as in Figure 3. First, *data or information* has to be *exchanged* between two IT systems. Second, the users of the two systems have to come to a *common understanding* based on that exchanged information, in this case, with respect to a certain cat and a certain mat.

[8] Reference 6

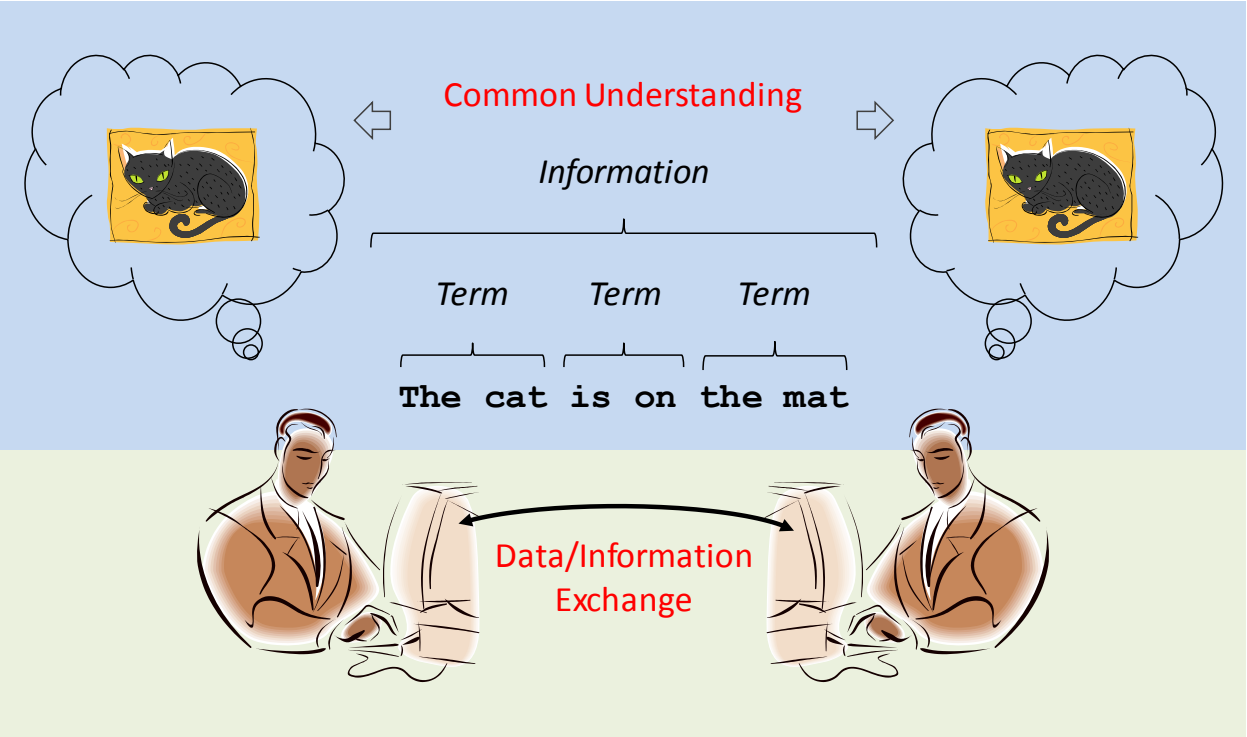

Figure 3. Illustration of the Definition of *Semantic Interoperability*

2.2 Data Collection Techniques

The approach to collecting data and information for this study was first to identify the key IT systems that are currently being used for COIN operations in Iraq and Afghanistan. Key IT systems include the Combined Information Data Network Exchange (CIDNE), the Command Post of the Future (CPOF), Tactical Ground Reporting (TIGR) system, Force XXI Battle Command Brigade and Below (FBCB2), and Joint Operations Intelligence Information System (JOIIS).

Once candidate systems were identified, a mapping of information flows among these systems was done to see what systems and what information was being exchanged among echelons of command from patrol to corps and coalition levels. This analysis allowed the study to focus initially on three major information systems, CIDNE, CPOF and TIGR, and later on, FBCB2 and one coalition system.

Contact was made with the CIDNE, CPOF, TIGR, FBCB2, and JOIIS program offices to better understand how these systems were used to collect and report information and share it with other systems. From these contacts, it was decided that SIGACT information would be appropriate to analyze for purposes of measuring semantic interoperability among systems.

SIGACT terminology used by each of the systems was then collected.

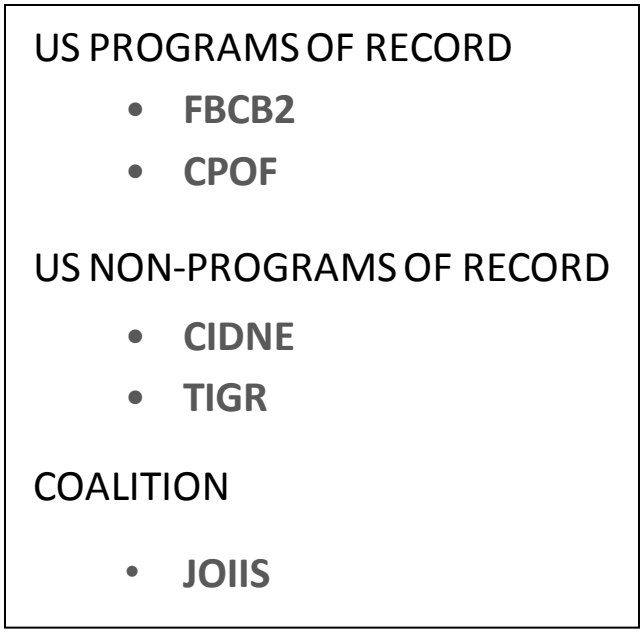

Figure 4. IT Systems Analyzed

The set of IT systems shown in Figure 4 above were chosen for semantic interoperability analysis.[9] These systems are key to providing and sharing information related to COIN Significant Activity reports (SIGACTs). Because SIGACT information is available in structured format with template lexicons, it is believed that this information can be more quickly analyzed for this study than other non-structured COIN information.

Note that this assessment of semantic interoperability is focused on "structured data" only. Unstructured data (for example, the free-text often used in comment fields) is also exchanged between the systems under review. But the very nature of unstructured data—its tendency to be ambiguous, vague, imprecise, and based on a large and uncontrolled vocabulary—did not permit a strictly quantitative assessment of semantic interoperability that was the principal objective of this study. Indeed, it could be argued that structured data in IT systems is a necessary condition of robust semantic interoperability. Be that as it may, metrics for measuring semantic interoperability among IT systems that use primarily unstructured data (e.g., intelligence systems) merit similar research.

2.3 Semantic Interoperability Measured

Given that the terms (individual words) and the information (sentences) that can be obtained by combining words in meaningful groups seem to underlie both concepts of common understanding and data/information exchange, there are two straightforward ways to measure or determine the degree of interoperability for distinct systems with respect to terms and information. On the one hand, semantic interoperability can be measured with respect to the *terms* used by target systems—the terms found in the systems' data models. On the other

[9] These IT systems are described in Appendix B.

hand, semantic interoperability can be measured with respect to the *information* that can be conveyed by combining individual terms of the target systems' data models, which we call information-level semantic interoperability.

Two systems can be considered as *term-level semantically interoperable* to the extent that the terms of their corresponding lexicons (or data models) are common.[10] For instance, if the lexicon of system S_1 contains n distinct terms and the lexicon of S_2 contains m distinct terms and x terms of the two lexicons are common (have the same semantics), then the degree or extent of semantic interoperability between the two systems is $x/((n+m)-x)$. Perfect term-level semantic interoperability between two systems would be 1.[11]

Two systems can be considered as *information-level semantically interoperable* to the extent that the semantic statements composable from all terms of their corresponding lexicons are common. For instance, suppose the lexicon of system $\mathbf{S}_i$ contains n_i distinct subject terms, ($s_{i,j=1...ni}$), m_i distinct verb terms, ($v_{i,j=1...mi}$), and k_i distinct object terms, ($o_{i,j=1...ki}$). Suppose further that the rules for the semantic composition of these terms into statements expressing information is simply to concatenate the subject, verb, and object terms into statements of the form *s, v, o*. For system $\mathbf{S}_1$, there would then be $(n_1 \bullet m_1 \bullet k_1)$ possible statements (pieces of information expressible by $\mathbf{S}_1$). Suppose there is a similar situation for system $\mathbf{S}_2$ where the number of semantically meaningful statements (information conveying lexical entities) is $(n_2 \bullet m_2 \bullet k_2)$. Then the degree or extent of semantic interoperability between the two systems is $x/(((n_1 \bullet m_1 \bullet k_1) + (n_2 \bullet m_2 \bullet k_2))- x)$ where x is the number of instances of ordered-triples, $< s_{i,j}, v_{i,j} , o_{i,j} >$, in common (where the ordered-triple $< s_{i,j} , v_{i,j} , o_{i,j} >$, is a member of the set of the cross-product of the subject, verb, and object terms of the respective systems). For measuring the semantic interoperability among more than two systems, the expression is $x / (\sum (n_i \bullet m_i \bullet k_i) – x)$, where the summation is over the number of systems and x is the number of instances of ordered triples in common across the systems.

Figure 5 is an example of how term-level interoperability can be measured using two information systems having three terms in common. The single term-level of interoperability is calculated using the formula $x / ((n + m) - x)$. The number of terms in common, x, is 3; the total number of terms, $(n + m)$ is 10 (n is 6 and m is 4); the total number of *unique* terms, $((n + m) - x)$, is 7. Term-level semantic interoperability for the two example systems is then 3 / 7 = .43.[12]

[10] Terms are "common" if and only if they have the same semantics (i.e., the same meaning) *with respect to the underlying information systems that process the terms as well as the users who use the associated information systems*. For the most part we had to rely on orthographic similarity to infer semantic equivalence of terms that were superficially equivalent. None of the systems we examined in this study provided the rigorous definitional detail that we would have liked to have examined in order to be able to claim with full confidence that two terms meant exactly the same thing to their respective users.

[11] If two IT systems use *exactly* the same number of terms and those two sets of terms are equivalent, then $n = m = x$, and so $x/((n+m)-x)$ equals $x/((x+x)-x)$, which equals 1.

[12] It is assumed that these two systems are intended to be used for the same functionality or aspects of the operational mission, and that all of the terms of each system are needed for information exchange.

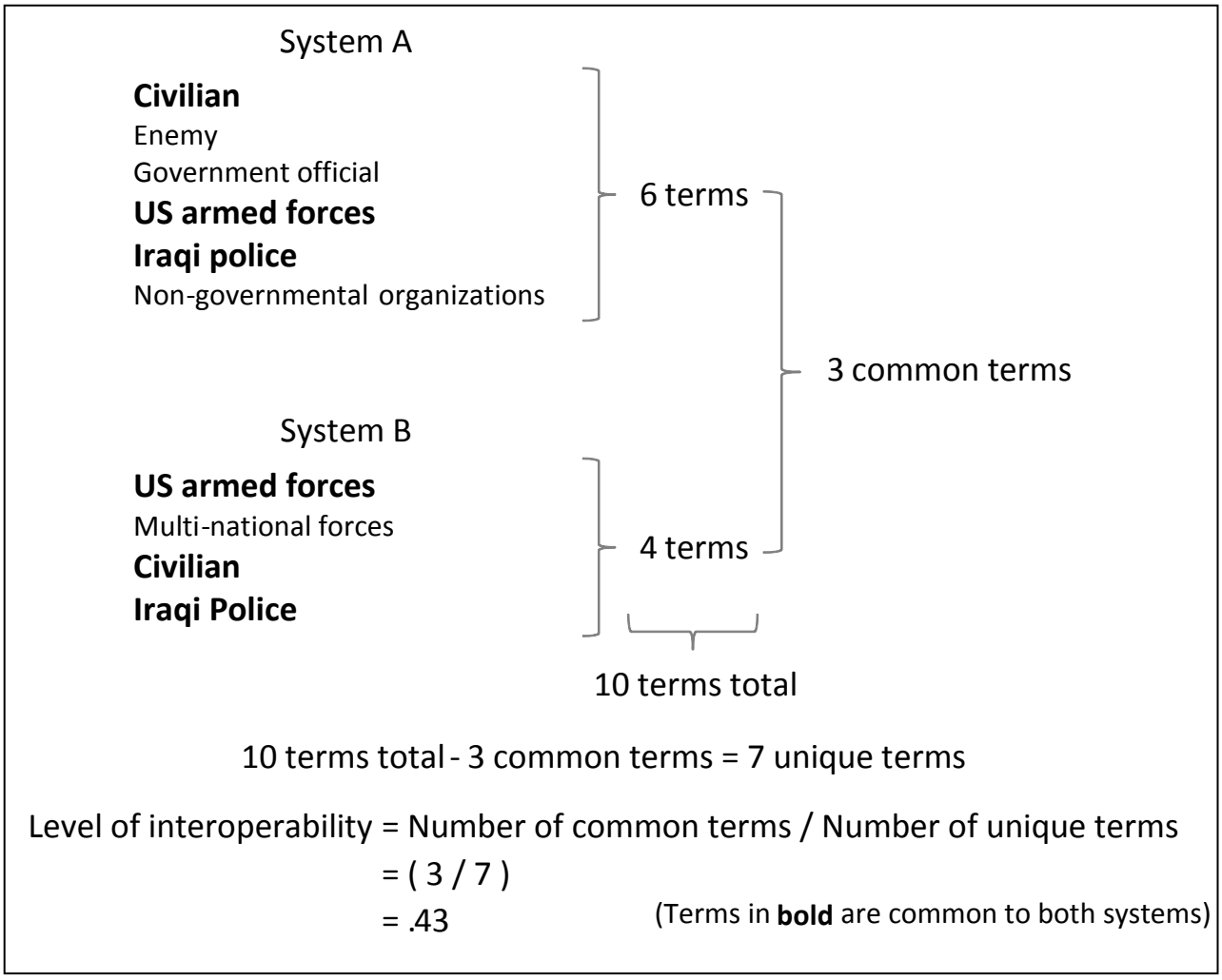

Figure 5. Example of *Term-Level* of Interoperability Measurement

Figure 6 illustrates semantic interoperability at the more relevant information level. The set of possible information (statements) one can assert within an IT system is the set of (semantically) coherent statements that can be produced by concatenating subject terms with predicate terms.[13]

[13] For this example, we are using the simpler two-place sentence template (subject-predicate) versus the three-place template, (subject-verb-object), and upon which our calculations are made below. We are also ignoring location (GEOLOC) and data-time-group (DTG) which would be an integral part of any such message.

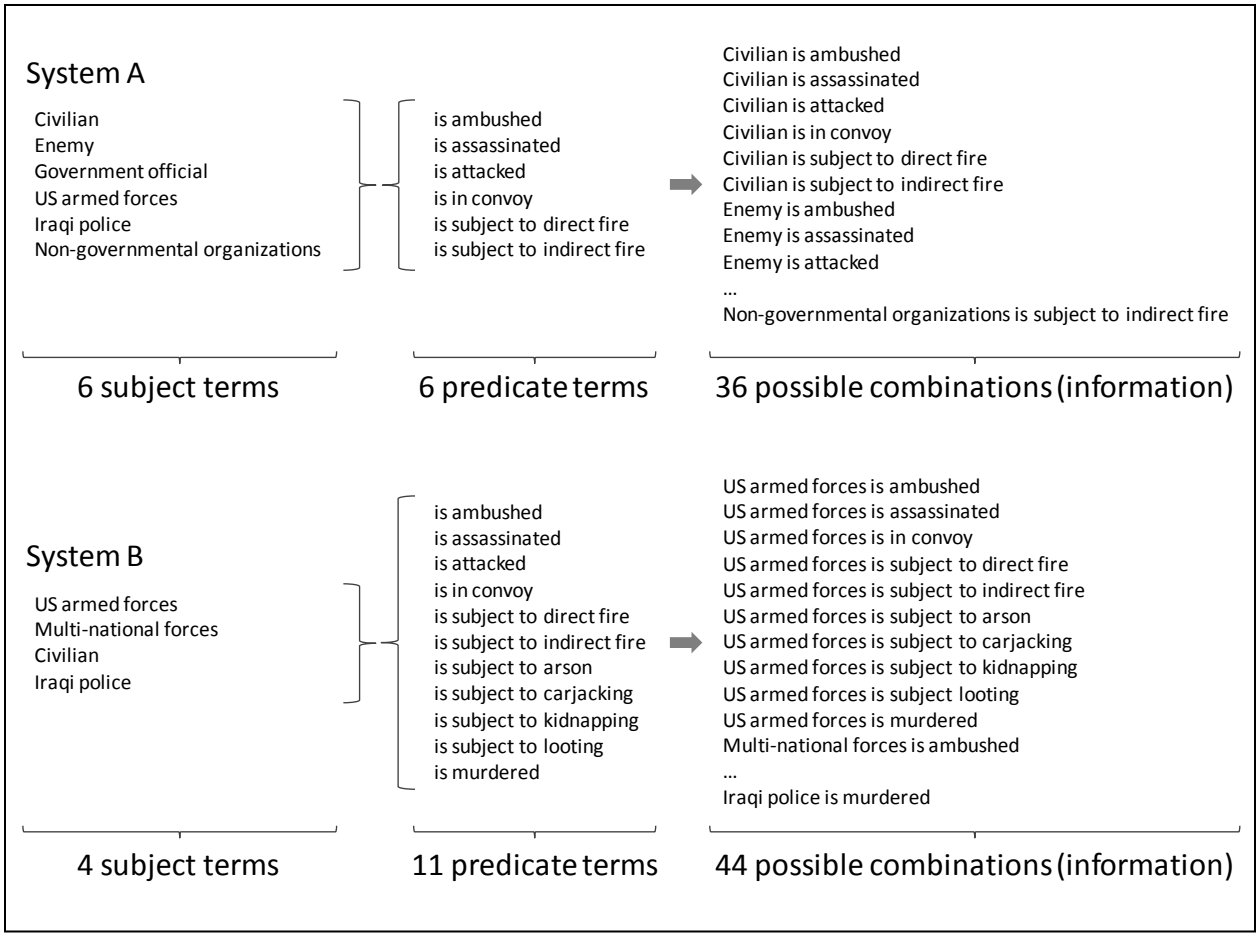

Figure 6. Example of *Information-Level* Semantic Interoperability

Assuming that each such concatenation is semantically coherent, the number of possible (assertable) statements (pieces of information) of System A is 6 subject terms times 6 predicate terms equals 36 subject-predicate concatenations, that is, possible statements of fact or pieces of information. Similarly, the number of possible (assertable) statements (pieces of information) of System B is 4 times 11 or 44. The total possible statements for both systems is 36 + 44 = 80.

The two systems have three subject terms in common (Civilian, US armed forces, and Iraqi police) and six predicate terms in common (i.e., all of the predicates of System A). Therefore, the number of shared (common) *possible* statements (information) is 18 out of a total possible domain of discourse of 80 possible statements. The information level of semantic interoperability is, accordingly, 18 / ((80) – 18) = .29. These simple calculations are illustrated in Figure 7.

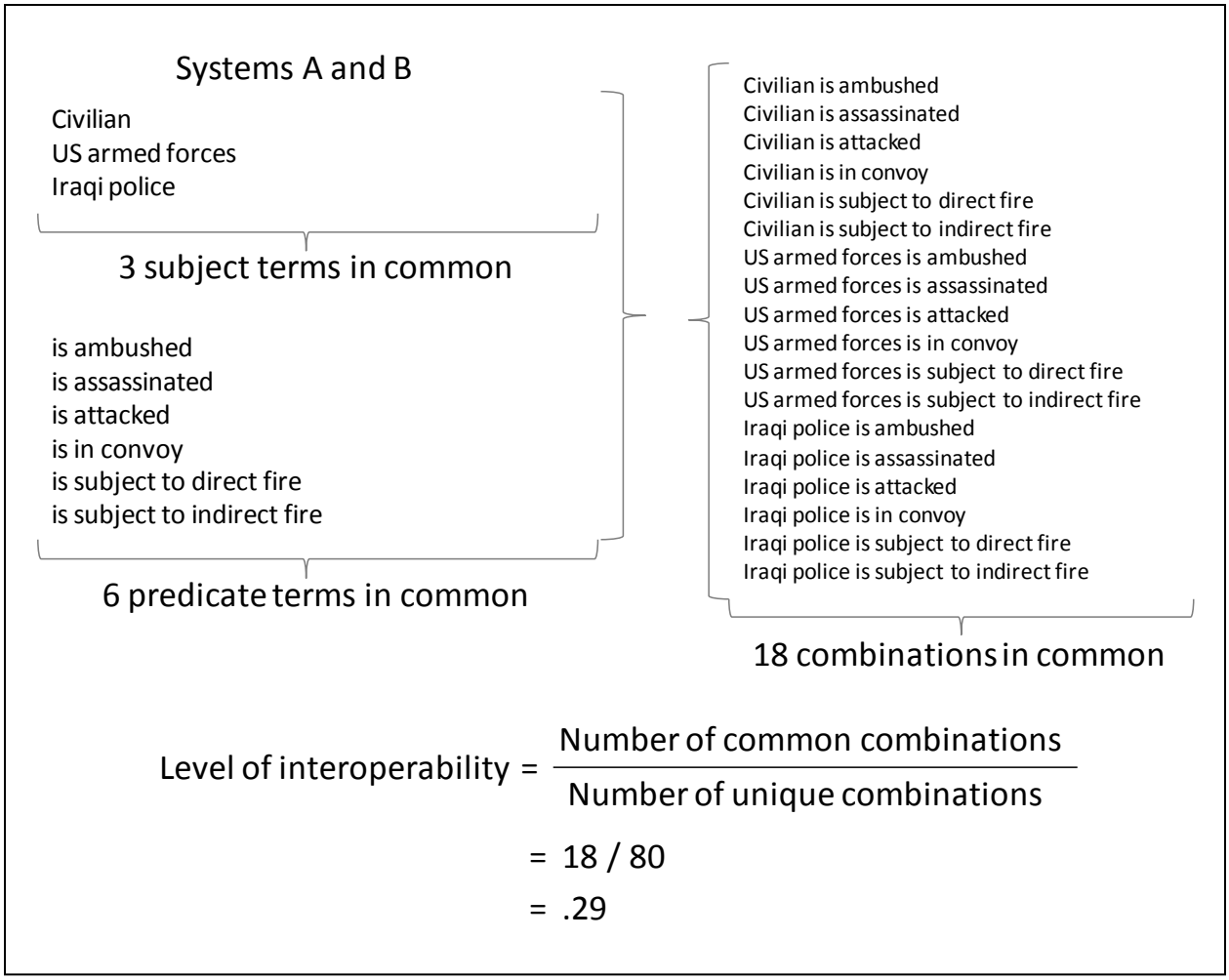

Figure 7. Measurement of *Information-Level* Semantic Interoperability

One way information can be formed is by combining a subject such as a person or group, an action verb such as attack, and an object such as the target of the action into a declarative sentence. Indeed, this is what users are really doing while not thinking about it as they select from various pull-down menus or click on check-boxes when entering information into IT systems (or even when they fill-out a written form). For example, Figure 8 is one of the first screens for entering an IED report into CIDNE.[14]

[14] Reference 7

See IDA Document D-4018 for FOUO material
https://wiki.kc.us.army.mil/wiki/Data_Product_Catalog

Figure 8. Sample CIDNE IED Reporting Screen

The CIDNE user fills in various fields (Date Discovered, MGRS, Call Sign, Reporting Unit) and then selects an Event Type from a pull-down menu. The result, when committed to the underlying database, is a conjunctive set of statements (pieces of information) not all that unlike the (notional) following:

{ $Unit_1$ *has Call Sign* = Firestorm 23 &
$Unit_1$ *has Reporting Unit* name = WIT Team 19 &
$Unit_1$ *reported* $Event_1$ *&*
$Event_1$ *Event Type* = IED Explosion &
$Event_1$ *occurred at* MGRS = 383MB123456 &
$Event_1$ *Discovered Date* = 28 Jan 2007 }

CIDNE has data categories that contain terms describing the types of units, event types and categories, and targets of attack. These categories can be mapped to the subject, the action verb, and the object or target to formally represent a piece of information. Figure 9 is a notional example of information from the SIGACT domain of discourse mapped to data categories and terms in CIDNE. If a warfighter were using CIDNE to report an anti-Iraqi forces VBIED attack on a host nation government official at a certain location and at a certain time, the warfighter would

select Anti-Iraqi forces, Enemy Action, IED explosion, and Government official from the pull-down menus that CIDNE provides.[15]

Figure 9. Information Example in the SIGACT Domain of Discourse

Comparison of the lexicons of four US C2 IT systems used for SIGACT reporting, namely CIDNE, CPOF, TIGR, and FBCB2, revealed relatively few common terms. Table 1, for instance, shows only seven instances of three-or-more matches between the terms used to report actions or activities.[16] Given that there are about 30 candidate categories—the 30 rows of the table—these seven instances of three-or-more matches represent only about a 25 percent success rate. The two-out-of-four match rate is considerably better, and the at-least-two-out-of-four match success rate begins to approach 100 percent. But what is this telling us? The take away here is that only two of these particular IT systems can actually share information about events

[15] CIDNE's representational capabilities are far more granular, of course. It implements most of version 1 of the Weapons Technical Intelligence (WTI) IED Lexicon and can capture the specific type of IED, namely, the vehicle -borne IED (VBIED) used in the example.

[16] Actually, the situation is worse. The entries listed under FBCB2 are those from the pull-down menus for reporting "equipment" (line 4 of the "spot report," the SPOTREP). The table also does not show the many other terms used in these systems to report actions or activities that appear to be unique. Complete results are presented in Appendix A.

of the same kind. Given that these event types are fairly basic to military operations (i.e., nothing very esoteric or specialized), the four systems used to report and share operational event information can do so with only half of the community of users.

See IDA Document D-4018 for FOUO material
https://wiki.kc.us.army.mil/wiki/Data_Product_Catalog

Table 1. Comparison of Action Terms in Four US C2 Systems[17]

Term-level comparison is admittedly a rudimentary measure of semantic interoperability. Information-level measurements are more refined. Table 2 illustrates a way to determine how much information—formed by combining terms corresponding to person/group, action, and

[17] The FBCB2 column requires a caveat. The list of actions (or activities) available on the pull-down menu for the activity entry on the FBCB2 SPOT report actually contains 14 entries (including No Activity). Only two of the FBCB2 selection choices for Activity match Action terms in the three other US systems under study. (The two matching terms are *Attacking* and *Reconnoitering*. The complete list of FBCB2 activities Is provided in Appendix A.) The list of selection options for Equipment on the FBCB2 SPOT report is being augmented to include the value displayed in the table under FBCB2 (except for Mortar). Since this Equipment field could be used to report certain specifics of an IED incident, we opted to use those values In the table, giving us a greater level of interoperability among other systems.

target data—can potentially exist in each COIN information system. The person/group category called *hostile* was chosen because it is common to the person/group category in CPOF and TIGR and corresponds to the Anti Iraqi forces category in CIDNE. The values in the first three columns are the number of terms found in each category. The number of possible combinations of the terms is shown in the fourth column. Assuming information is represented by a phrase or a sentence containing these terms, the number of combinations of terms can be thought of as a measure of information expressible in and processable by that system. The number of distinct hostile events (ignoring differences in time and location) that can be represented increases dramatically from FBCB2 to CIDNE to CPOF to TIGR.

	Person/Group	Action	Target	Information
FBCB2	1	14	12	168
CIDNE	1	37	6	222
CPOF	1	66	8	528
TIGR	1	20	44	880
JOIIS	1	32	21	672

Table 2. Term and Information Counts for Three US Systems and One Coalition[18] System

The degree of information-level interoperability among these IT systems was determined from the number of common term combinations expressing information and the number of possible ways corresponding terms can be combined according to the formula described at the beginning of the measuring semantic interoperability section of the report. Table 3 presents information-level interoperability measurement results for three US SIGACT-processing systems. The first three rows of the table show pair-wise interoperability. The last row shows three-way interoperability. (It is important to note that the interoperability measured here is only for one type of information based on persons, actions, and targets and not an overall measurement of interoperability among the systems.)

[18] Reference 8

	Person/Group	Action	Target	Common Information	Degree of Interoperability
CIDNE - CPOF	1	16	2	32	.04
CIDNE - TIGR	1	12	1	12	.01
CPOF - TIGR	1	11	1	11	.008
CIDNE - CPOF -TIGR	1	4	1	4	.002

Table 3. Example of Measuring Information Interoperability for Three US SIGACT-Processing Systems

Table 4 presents the results of determining the degree of information-level interoperability between three US systems (one pair at a time) and one major coalition system, JOIIS. The last row of the table looks at the degree of interoperability of all four systems collectively.

	Person/Group	Action	Target	Common Information	Degree of Interoperability
JOIIS - CPOF	1	8	3	24	.04
JOIIS - TIGR	1	5	1	5	.02
JOIIS - CIDNE	1	11	3	33	.003
JOIIS – CIDNE – CPOF -TIGR	1	2	1	2	.001

Table 4. Example of Measuring Information Interoperability for US Systems and One Coalition System

2.4 Semantic Interoperability in Networked Systems

The Open Systems Interconnection Reference Model (OSI Model), shown in Figure 10, illustrates where the focus of semantic interoperability examined in this study lies with respect to the various layers of communications and computer network functionality. Each layer in the model provides services to the layer above it and receives services from the layer below it. The degree of semantic interoperability among IT systems is determined mainly at the application and presentation levels. It is only at the application and presentation layers of an IT system that data is presented to a user in a form designed for immediate understanding and comprehension.

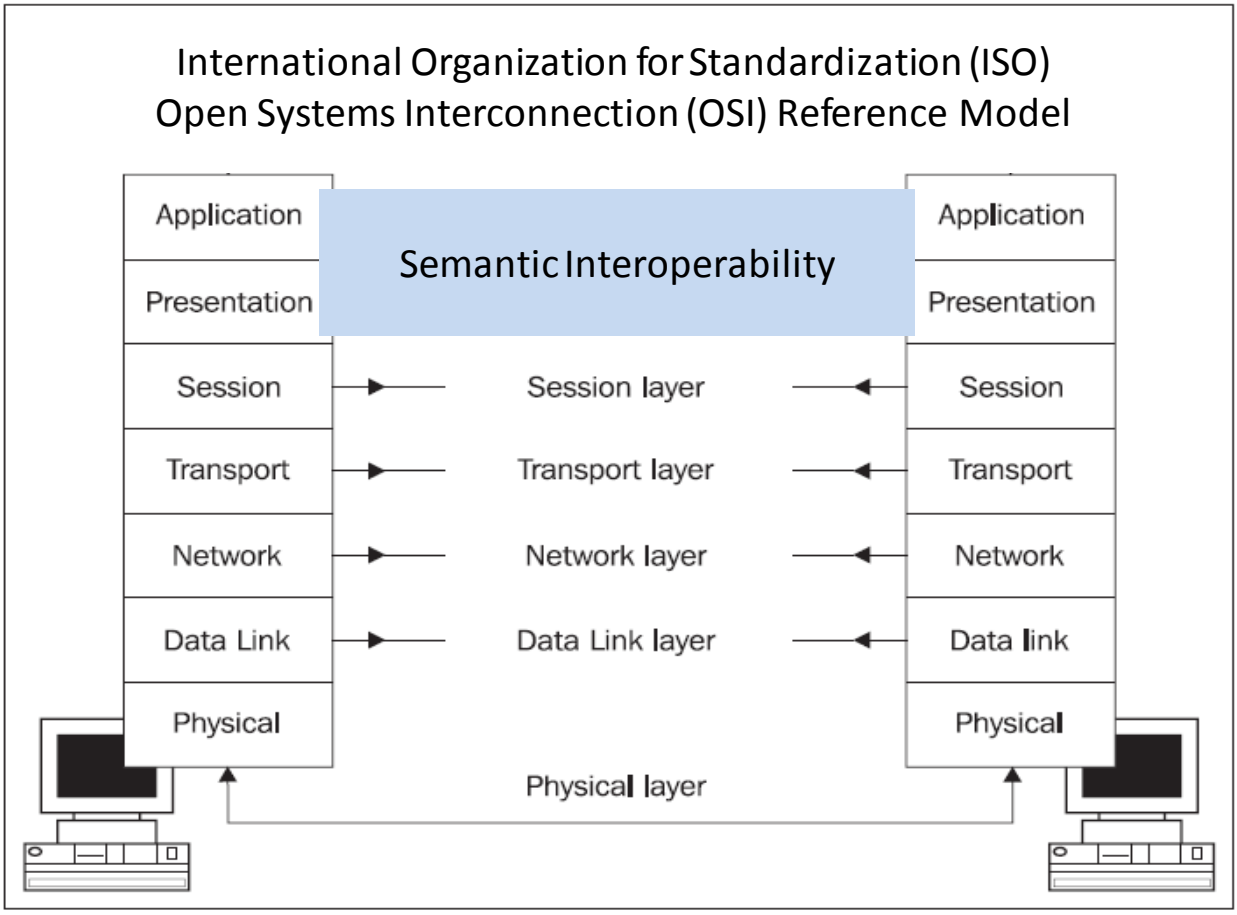

Figure 10. Semantic Interoperability in Networked Systems

2.5 Semantic Interoperability and Information Flow

While we did not quantitatively assess the effects on semantic interoperability of data exchange at the OSI layers below the application and presentation layers, the complexity of data exchange among current systems may contribute to the overall interoperability problem. The sheer number of different systems involved and the complexity of the data exchange mechanisms between them undoubtedly impedes timeliness, accuracy, and completeness of

information exchange between command echelons. Figure 11 may give the reader some feel for the complexity of existing flows of IED data among US tactical-level systems.[19]

Figure 11. Complexity of IED Information Flows

[19] Reference 9

3. Analysis of Barriers to Data Interoperability

This section describes the results of analysis of key factors that determine the degree of semantic interoperability among warfighter information systems in the larger sense alluded to earlier: doctrine, information understanding, leadership, ability, and information exchange.

The findings are presented in three columns as shown in Figure 12. The first column, Area of Analysis, describes the particular area of the overall analysis in which raw data was collected. The Results column presents significant results (e.g., trends, averages, logical entailments, etc.) obtained from the *analysis* of the raw data. The final column, Implications, lists the significant repercussions in terms of future states-of-affair if current conditions are not changed and are allowed to continue.

3.1 Doctrine

Area of Analysis	Results	Implications
Army and Joint Publications	Doctrine for counterinsurgency operations exists in FM 3-24, FM 3-24.2, and JP 3-24	Doctrine needs to be more extensively mapped to information technology systems for automated use in counterinsurgency operations

Figure 12. Findings with respect to Doctrine

Doctrine for conducting counterinsurgency operations exists in both Service and Joint publications.[20] As indicated in Figure 12, comparison of these publications with several systems used to process SIGACT information revealed that much of the doctrinal terminology and associated processes is not reflected in warfighter IT systems. Rather than reinforcing doctrinal training—and the best practices and lessons learned that doctrine is intended to institutionalize—today's warfighter must contend with an array of computer tools that in effect provide different, if not altogether contrary, doctrine and reduce the warfighter's effectiveness, particularly with respect to information management.

[20] Reference 10

3.2 Information Understanding

Area of Analysis	Results	Implications
Terminology	Only a small percentage of the total possible "information" (defined as the grammatical combination of available terms) is common among the C2 systems analyzed; problems of semantic interoperability are at the application/presentation levels of IT systems.	Poor semantic interoperability will continue to limit the benefits of automation to the warfighter until semantic alignment (harmonization)—in accordance with CJCSI 5702.01C which prescribes the standardization of "military and associated terminology" -- is obtained at the application/ presentation levels of IT systems.
Reporting "formats" for violent events (e.g., SIGACTS)	The reporting "formats" (including the available options in reporting tool "drop-down" lists) differ widely among US and coalition C2 systems.	The lack of standard and uniform IT implementations of standard reports (e.g., the SPOT report) is a key factor contributing to the semantic interoperability problem.
Interoperability validation/accreditation process	The JCIDS process for validating interoperability of IT acquisitions relies only on developer assurances; the process does not examine semantic interoperability at all; some non-PORs are fielded without interoperability accreditation.	Without a meaningful validation/ accreditation process for semantic interoperability there is risk that deployed IT systems will not be fully interoperable.

Figure 13. Findings with respect to Information Understanding

With respect to terminology (row 1 of Figure 13), the measurement of the common terminology and possible information that can be formed from that terminology showed that only a small percentage was common among CIDNE, CPOF, TIGR, and FBCB2 systems.

With respect to reporting formats (row 2 of Figure 13), the formats used in SIGACT information systems vary widely, making it even more difficult to mediate information sharing (e.g., by mapping or translating terminology between systems) among those systems.

With respect to interoperability validation and accreditation (row 3 of Figure 13), the process used by the Joint Staff to validate that IT systems meet needed requirements does not take into account the intended *understanding* of exchanged information (semantic interoperability). This could render the accreditation process largely irrelevant with respect to the ultimate touchstone of net-centricity: common understanding.[21]

[21] Reference 11

Area of Analysis	Results	Implications
Mediation tools	The PASS server is the principal tool used to enable interoperability among systems in the ABCS portfolio; the SIGACT "topic" is the primary vehicle for exchanging violent event information; the fields of the SIG-ACT "topic" concerned with event descriptions or categorizations are only (size-limited) free-text fields with allowable values prescribed only by the originating system (e.g., FBCB2, CPOF); PASS does not attempt any data mediation (mapping and/or translation) between the deffering sets of terminology used by the ABCS suite.	Unless non-interoperability among ABCS systems is addressed at a more fundamental level (by aligning the systems to a common vocabulary), PASS will continue to be considered—mistakenly—the preferred vehicle for interoperability among major US C2 systems.

Figure 14. Findings with respect to Information Understanding (Cont'd)

In terms of mediation tools (Figure 14), the Publish and Subscribe Service (PASS), that is, the vehicle used for information exchange within the Army Battle Command System (ABCS), does not interpret or translate information from one system to another based on any predefined mapping table. Accordingly, unless the Army addresses the ABCS systems' non-interoperability at a more fundamental level (by aligning the systems to a common vocabulary), PASS will continue to be an unacceptable vehicle for interoperability among major US C2 systems.

3.3 Information Exchange

Area of Analysis	Results	Implications
IT systems	Tactical Operation Centers (TOCs) use different suites of IT systems; not all systems are available at all TOCs; TOC system configurations are not fully net-centric, preventing access to all important data.	The non-netcentric configuration of the IT systems deployed in various TOCs will continue to impede information exchange (sharing) among warfighters.
Communications	Information is exchanged between IT systems via telephone, radio, Web interfaces, and tactical (unclassified) and operational (classified) Internet using a variety of "middleware" (e.g., PASS, "multi-cast," "swivel chairs," "sneaker-net"); this plethora of communication techniques is needed to enable data sharing in the non-integrated, non-netcentric configuration of systems currently in use in the TOCs.	Reliance on existing methods for exchanging information will continue to impede the timely, accurate, and complete sharing of important information.

Figure 15. Findings with respect to Information Exchange

With respect to IT systems (row 1 of Figure 15), the difficulty in sharing information among existing IT systems in theater is due to the lack of a net-centric environment.[22] That is, data and information necessary to develop a comprehensive view of an event are not easily accessible to all automated systems.

Furthermore, the variety of communication channels, most of which use their own standards, introduces a complexity that results in less timely, less accurate, and incomplete information sharing.

Tactical Operation Centers (TOCs) use different suites of IT systems; not all systems are available at all TOCs; TOC system configurations are not fully net-centric, thereby preventing access to all important data.

With respect to communications (row 2 of Figure 15), information is exchanged between these systems via telephone, radio, Web interfaces, and tactical (unclassified) and operational (classified) Internets, while using a variety of "middleware" (e.g., PASS, "multi-cast," "swivel

[22] Reference 11

chair," "sneaker-net")[23]; this plethora of communication techniques is needed to enable data sharing in the non-integrated, non-net-centric systems currently in use in the TOCs.

The non-net-centric systems deployed in various TOCs will continue to impede information sharing among warfighters.

Reliance on existing methods for exchanging information will continue to impede the timely sharing of important information.

Area of Analysis	Results	Implications
Message formats	Many different message formats are used: Variable Message Format (VMF) messages (~ 50); PASS "topics" (~ 12); unique point-to-point data transfers (e.g., TIGR-to-CIDNE patrol reports). The semantic content of these messages differs as well.	Different message formats for exchanging information between systems—while perhaps necessary—increase the complexity of data exchange and will continue to jeopardize good semantic interoperability.
Data entry and data exchange procedures	Initial SPOT (SALUTE) reports (that may become SIGACT reports) are entered at multiple echelons (e.g., CO, BN, BCT, etc.); updates (additions, corrections) to SIGACTs can occur at any echelon.	Without tactics, techniques, and procedures (TTPs) that guide the systematic, uniform, and methodical entry and exchange of information there is no way to establish or maintain authoritative data.
	Exchanges can take from minutes to weeks depending on the data entry procedure and the system used for reporting.	The lack of information reaching the warfighter in a timely manner increases mission risk.

Figure 16. Findings with respect to Information Exchange (Cont'd)

With respect to message formats (row 1 of Figure 16), the lack of standard message formats contributes to the need for mapping and translation systems to understand the information exchanged among existing IT systems.

The tactics, techniques, and procedures (TTPs) used to report and share IED information contained in SIGACTS are not organized in a standardized fashion. A number of documents, including draft concepts of operations (CONOPS), describe the procedures as they exist, not as they should be for efficient reporting and access.

[23] "Multi-cast" refers to simultaneous transmission of data to many separate IT systems; "swivel chair" refers to manual reentry of data from one IT system to another; "sneaker-net" refers to transferring data from one information system to another using physically removable media such as thumb drives.

Many different message formats are used: Variable Message Format (VMF) messages (about 50 different kinds); PASS "topics" (about 12 different kinds). There are unique point-to-point data transfers (e.g., TIGR patrol reports to CIDNE). The semantic content of these messages differs as well.

Using different message formats for exchanging information between systems—while perhaps necessary—increases the complexity of data exchange and will continue to jeopardize the attainment of good semantic interoperability.

With respect to data entry and data exchange procedures associated with SIGACTS (row 2 of Figure 16), initial SPOT (SALUTE) reports are entered at multiple echelons (e.g., company, battalion, brigade combat team, etc.). These initial, typically tactical-level reports, may become SIGACT reports. SIGACT report updates (additions, corrections) can and do occur at any echelon.

Without TTPs that guide the systematic, uniform, and methodical entry and exchange of information, there is no way to establish or maintain authoritative data.

Exchanges can take from minutes to weeks depending on the data entry procedure and the system used for reporting.

The lack of information reaching the warfighter in a timely manner increases mission risk.[24]

[24] Reference 12

3.4 Leadership

Area of Analysis	Results	Implications
Command and control	Commanders have the discretion to employ whatever tools they feel are needed to accomplish their assigned missions. Many commanders do not feel that existing programs of record (PORs) are adequate for their information management purposes, and, accordingly, do not prescribe their use by their subordinates. Non-PORs (e.g., CIDNE and TIGR) are developed and fielded outside of the normal acquisition process. Individual warfighters also use a wide array of non-POR systems, including simple office automation tools—email, MS PowerPoint, MS Word, and MS SharePoint—personal log books, paper maps, wall charts, etc., to support their C2 information sharing and management needs.	If commanders are not provided the PORs they need to accomplish their missions, they will continue to procure non-PORs and ignore the PORs that continue to be developed at a not insignificant cost. Individual warfighters will continue to rely on a plethora of non-integrated "point solutions" to address their C2 information needs.

Figure 17. Findings with respect to Leadership

With respect to leadership (Figure 17), it is important to reiterate that commanders have the discretion to employ whatever tools they feel are needed to accomplish their assigned missions. However, many commanders do not feel that existing programs of record (PORs) are adequate for their information management purposes and, accordingly, do not require their subordinates to use them. Non-PORs (e.g., CIDNE and TIGR) are developed and fielded outside of the normal acquisition process. Individual warfighters use a wide array of non-POR systems, including simple office automation tools—email, MS PowerPoint, Word, and SharePoint—and personal log books, paper maps, wall charts, etc., to support their C2 information sharing and management needs.

If commanders are not provided with the PORs they need to accomplish their missions, they will continue to procure non-PORs and ignore the PORs that continue to be developed at a not insignificant cost. Individual warfighters will continue to rely on a plethora of non-integrated point solutions to address their C2 information needs.

3.5 Ability

Area of Analysis	Results	Implications
Individual Warfighter Ability	There is no evidence that individual warfighters lack the ability and will to carry out mission assignments in accordance with existing doctrine and the training they received prior to deployment. The will and ability to employ whatever means are available to share information is well documented.	Warfighter information that is only collected and shared face-to-face, by email, PowerPoint slides, radio or telephone cannot be readily aggregated and analyzed for trend or similar kinds of operational-level and strategic-level analyses. Widespread use of an array of tools that do not require the use of standard vocabularies for the capture and reporting of significant activities will continue to hinder the generation of user-defined common operational pictures and the achievement of the common understanding needed by the warfighter.

Figure 18. Findings with respect to Individual Warfighter Ability

With respect to individual warfighter ability (Figure 18), there is no evidence that individual warfighters lack the ability and will to carry out mission assignments in accordance with existing doctrine and the training they received prior to deployment. The will and ability to employ whatever means are available to share information is well documented.

Warfighter information that is only collected and shared face-to-face or by email, PowerPoint slides, radio, or telephone cannot be readily aggregated and analyzed for trend or similar kinds of operational and strategic analyses. Widespread use of an array of tools that do not require the use of standard vocabularies for the capture and reporting of significant activities will continue to hinder the generation of user-defined common operational pictures and the achievement of the common understanding needed by the warfighter.

4. Recommendations to Improve Data Interoperability

With respect to the key factors that affect semantic interoperability, we recommend that the following specific recommendations be adopted and implemented.

4.1 Doctrine

- Make the development of rigorously defined lexicons (unambiguous structured data) a central feature of warfighting doctrine. The "WTI IED Lexicon," for example, needs to be incorporated into doctrine that addresses COIN (e.g., Army Field Manual (FM) 3-24 (Counterinsurgency) and FM 3-24.2 (Tactics)
- Make the development and publication of official doctrine (e.g., C-IED) a priority; accelerate the development of doctrine that directly affects warfighting and that is supported in IT systems

4.2 Information Understanding

- Ensure that deployed (and deploying) IT systems use common data models (or mediation services), thus satisfying one necessary condition for semantic interoperability
- Ensure that IT systems incorporate, mirror, or otherwise fully embody the language of doctrine at the semantic level using structured data. To this end, iterate the development of doctrinal products in such a way as to eventually produce artifacts (e.g., Joint Publications) whose conceptual clarity, precision, and detail in the description of processes and terminology can be used to develop any IT system the doctrine needs to instantiate; close the communication's gap between doctrine writers and IT system developers so that the latter build the information technology defined by the former
- Develop a concept of operations (CONOPS) and implementing TTPs that formalize and standardize event reporting and report formats at all command echelons, particularly at the tactical level

4.3 Information Exchange

- Reduce the complexity of the information exchange process by reducing the number of different systems and communications processes used to effect information sharing
- Foster efficiency and greater levels of semantic interoperability by building IT systems that predominantly use structured data rather than unstructured (free text) data

4.4 Leadership

- Ensure that information processing requirements originate from the warfighter and that IT systems are made available to all relevant command echelons

- Monitor the use of IT systems by commanders to determine if they are being used and used properly. If these IT systems are not being used, determine why not and how best to ensure that IT systems acquisition can better support the warfighter

4.5 Ability

- Merge training in doctrine and training in the use of applicable IT systems into a single training package and train warfighters in doctrine and its supporting IT systems concurrently
- Ensure that the automated tools do not create additional burdens on the warfighter

5. Suggested Follow-on Activities and Further Studies

During the course of this study, we met (or otherwise communicated) with representatives of a number of organizations concerned with interoperability and/or with responsibilities for different aspects of the interoperability issue. Based on these interactions, topics for further research include:

5.1 Doctrine

Discussions with Army Training and Doctrine Command (TRADOC), Joint Staff Command, Control, Communications, & Computer Systems (J6), and the Joint IED Defeat Organization (JIEDDO) led to increased awareness of the need to codify IED standard terminology into counterinsurgency doctrine.

5.2 Information Understanding

We are continuing to explore with Army CIO/G-6 and JIEDDO how to apply metrics developed in this study to a more broad set of services that can help assess the use of standard lexicons in counterinsurgency information systems.

5.3 Information Exchange

We have initiated an effort to assist the JIEDDO in standing up a Weapons Technical Intelligence (WTI) task force that, in part, will focus on information sharing in the Afghanistan theater of operations.

5.4 Suggested Further Studies

Studies relevant to implementing this study's recommendations include:

- A study to devise good methodologies and automated capabilities to enable the technical, cost/benefit, and programmatic analyses of Capability Sets and related initiatives that address the interoperability problems uncovered in the current study. A pilot prototype is needed to enable the delivery of IT systems—in months, not years—to achieve effective interoperability and collaboration.
- A study of the governance and training processes to ensure that all IT systems are interoperable. Individual COIN information systems such as CIDNE, CPOF, TIGR, and FBCB2 each have governance processes and training procedures, but these processes and procedures are not viewed from an enterprise perspective. Organizations external to the Army and beyond the Army's control are publishing and fielding relevant documents (guidance, lexicons, doctrinal publications) and IT systems that the Army is

incorporating into its operations. The impact of this enterprise (joint) approach to the semantic interoperability of its IT systems has to be examined.

- A study to examine and document the factors that commanders consider when they select the IT for their forces to use, particularly with respect to current C-IED operations in current OCOs. These factors include the responsibilities and authority of commanders, the fact that doctrinal publications are the authoritative guidance on warfare terminology and processes, and the fact that C2 is basically about human interactions. IT intended for use in C2 must enhance, not impede, the flow of information between warfighters and facilitate implementation of the doctrinal processes. It is important to understand that commanders' selection of IT for use in a particular combat situation is completely separate from the governance process that regulates IT development. This can be seen in US Central Command's direction to use CIDNE rather than Service PORs.
- A study of how to transition from current separate hardware-based systems to data-centric information sharing, leveraging legacy equipment
- A study of how evolving warfighter requirements can easily be adopted and incorporated into existing PORs

6. Summary

- The study examined the degree of semantic interoperability that is currently possible among four US systems and one coalition system with respect to COIN and C-IED operations
- The methodology devised for measuring semantic interoperability is applicable to any domain, not just COIN and C-IED
- ***The fundamental finding was that semantic interoperability***—defined as the ability to achieve common understanding of shared information—***among information systems that process COIN- and C-IED-related SIGACT reports is marginal, at best***
- The lack of robust semantic interoperability appears to be because of a large disconnect
  - Between system developers and warfighters: developers are not delivering the solutions the warfighters want and need
  - Between system developers and the developers and publishers of warfighting doctrine
- The Army needs to develop and implement a (better) process that ensures
  - Information requirements originate from and solutions are directed to the warfighter, at all command echelons
  - Information solutions incorporate, mirror, or otherwise fully embody the language of doctrine, at the semantic level

Appendix A – Analysis Detail

A-1. FBCB2 – Representational Scope

Figure 19 depicts the terminology available in FBCB2 for submitting a SPOT report. The four IED-related terms under the "Equipment 1: Target" heading (viz., IED, VBIED, Suicide Bomber, and IED Explosion) are new options just now being tested for future fielding.[25]

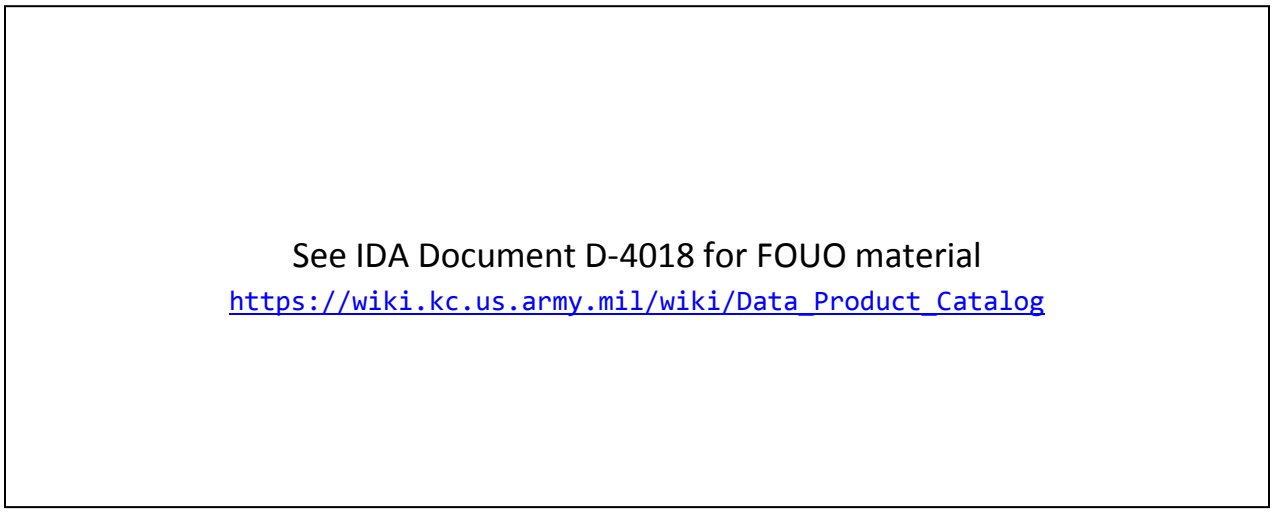

Figure 19. FBCB2 Representational Scope

A-2. CPOF – Representational Scope

Figure 20 depicts the representational scope of CPOF for "Hostiles." It provides a concise view of all possible "person/group—action—target" reports that can be conveyed using CPOF when the person/group is a hostile. For example, the CPOF terminology allows the message "Hostiles HIJACKING (VEHICLE) CIVILIAN" to be generated to report that a civilian vehicle was hijacked by a hostile person or group.[26]

[25] Reference 13
[26] Reference 14

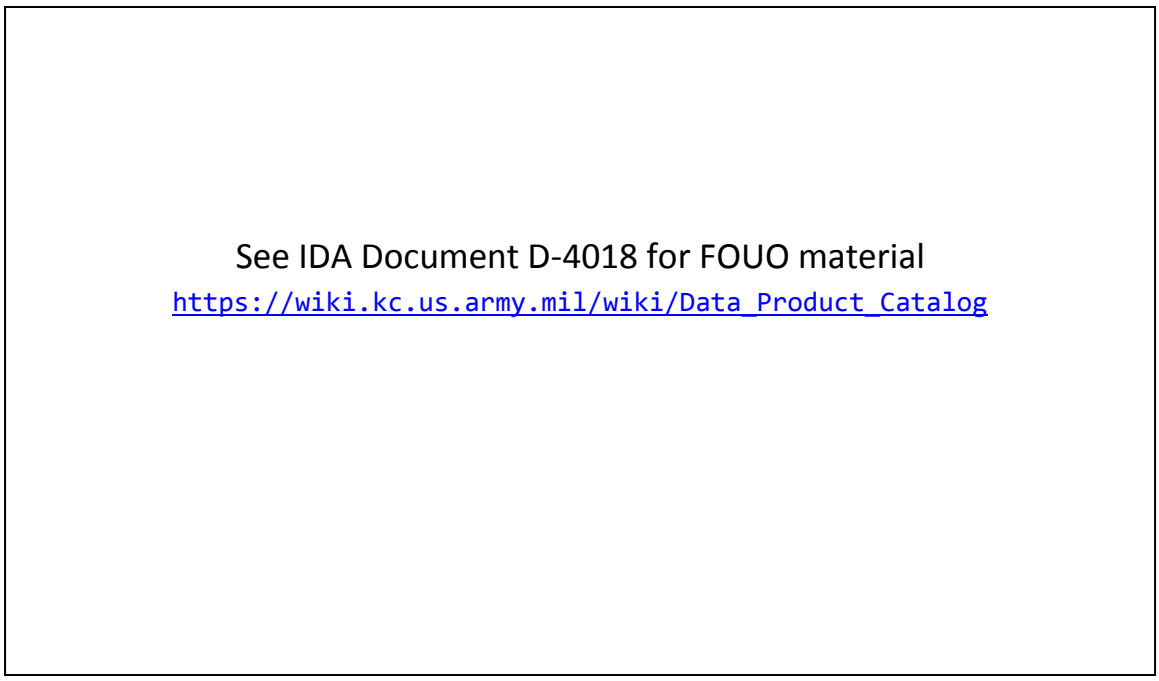

Figure 20. CPOF Representational Scope (Hostiles)

A-3. TIGR – Representational Scope

Figure 21 depicts the representational scope of TIGR for "Hostile." Figure 22 shows the terminology used in TIGR for the two non-hostile categories, "Friendly" and "Locals."[27]

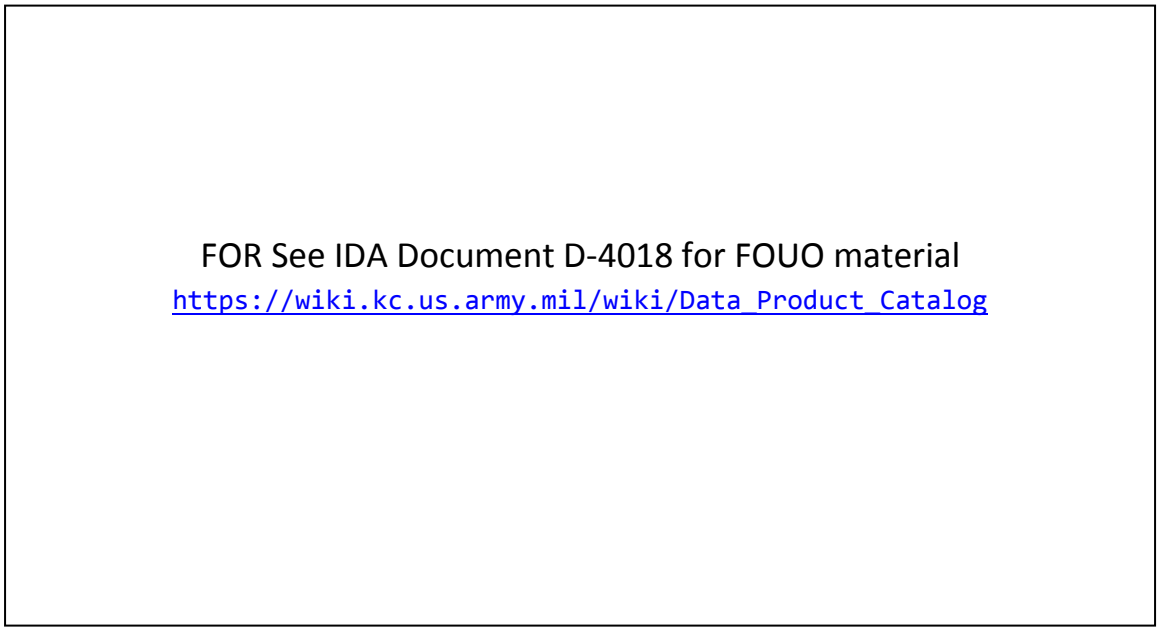

Figure 21. TIGR Representational Scope (Hostiles)

[27] Reference 3

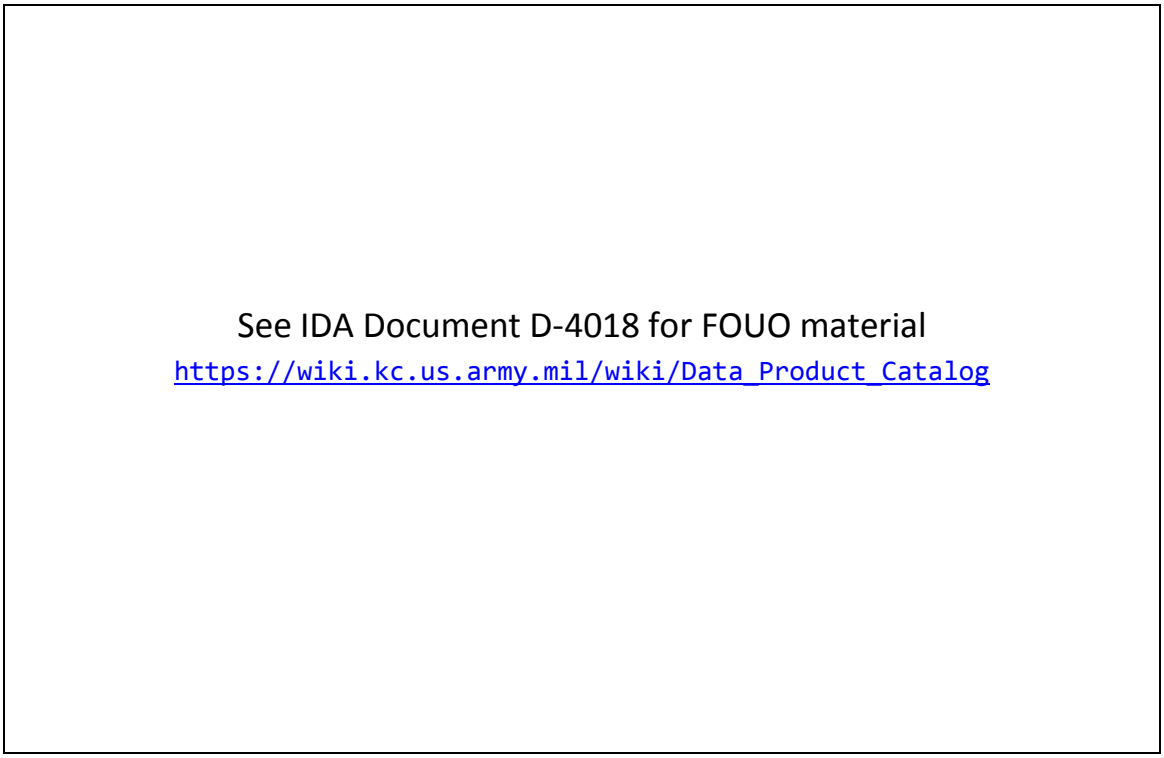

Figure 22. TIGR Representational Scope (Friendly and Locals)

A-4. CIDNE – Representational Scope

Figure 23 depicts the representational scope of CIDNE for "Hostiles." Note that there are several sub-categories of hostiles (e.g., Anti-Iraqi Force, Insurgent, etc.). Note also that CIDNE provides for more detailed characterization of actions via the Action Mode concept. This is particularly useful in characterizing the method of deployment of IEDs in IED incidents.[28]

[28] Reference 7

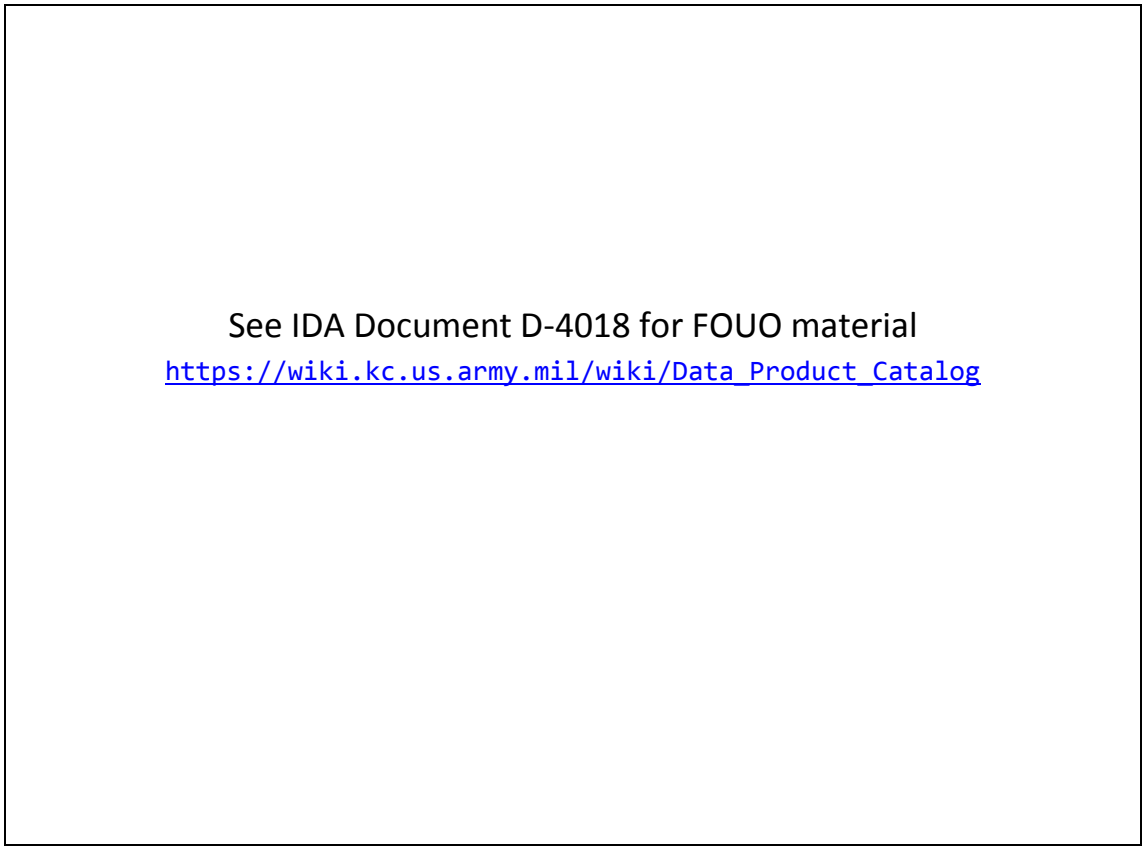

Figure 23. CIDNE Representational Scope (Hostiles)

A-5. Terminologies for Action with no Common Terms

Figure 24 depicts the terms available for reporting activity (actions) that have no counterparts among the four principal C2 systems examined.

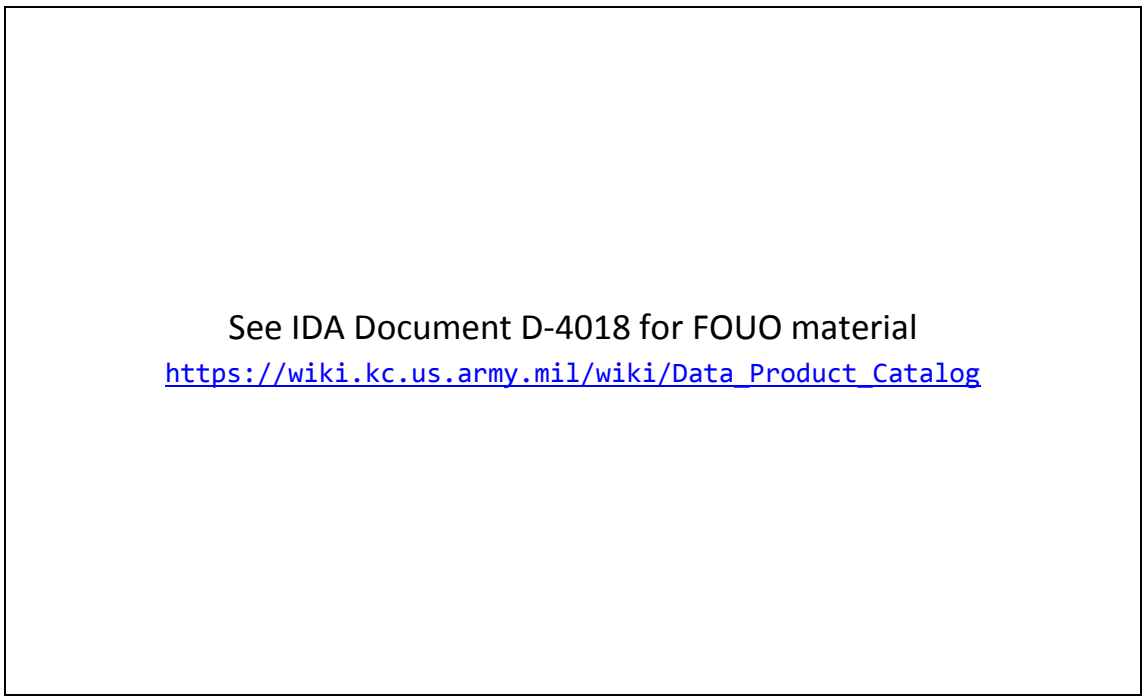

Figure 24. Terminologies for Action with no Common Terms

Appendix B – IT Systems Examined

B-1. FBCB2

Force XXI Battle Command Brigade and Below (FBCB2) is a communication platform designed for commanders to track friendly and hostile forces on the battlefield. FBCB2 is a digitized information system that provides on-the-move, real time and near-real-time battle command information to tactical combat, combat support, and combat service support leaders and soldiers.

B-2. CPOF

Command Post of the Future (CPOF) is a C2 software system that allows commanders to maintain topsight over the battlefield; collaborate with superiors, peers and subordinates using live data; and communicate their intent. CPOF provides the user capability to simultaneously collaborate and share data among operators at the same echelon and also between operators at other echelons in real-time. CPOF supports the Commander's battle management and information operations by rapidly processing and displaying combat information from other supporting Army Battle Command Systems (ABCS).

B-3. TIGR

TIGR is a multimedia reporting system for soldiers at the patrol level, allowing users to collect and share information to improve situational awareness and to facilitate collaboration and information analysis among junior officers. The system allows soldiers and Marines at the patrol level to collect and share information to improve situational awareness and to facilitate collaboration and information analysis among junior officers. TIGR is particularly suited to counterinsurgency operations and enables collection and dissemination of fine-grained intelligence on people, places, and insurgent activity. Being focused on users at Company level and below, TIGR complements existing reporting systems that focus on the needs of users at Battalion or Brigade level and above.

B-4. CIDNE

The Combined Information Data Network Exchange (CIDNE), a secure internet host site, contains an engagement tool for tracking three types of entities: people, facilities and organizations. In military terms, these entities are referred to as spheres of influence. CIDNE provides an end-to-end knowledge management solution in support of Counter-Improvised Explosive Device (C-IED) operations. Capabilities support both defeating the device and attacking the network--from initial threat reporting through device exploitation, target development and evidence tracking. The IED report implements the Weapons Technical Intelligence (WTI) lexicon standard.

B-5. JOIIS

See IDA Document D-4018 for FOUO material

https://wiki.kc.us.army.mil/wiki/Data_Product_Catalog

Appendix C – References

(1) Department of Defense Dictionary of Military and Associated Terms (Joint Publication 1-02), 12 April 2001 (as amended through 13 June 2007).

(2) Moore, Lt Col David M., USA, "Battle Command Software: Meeting the Commander's Needs?," US Army War College Report, March 15, 2006.

(3) McDonald, R., Greene, H., Project Manager and TRADOC Capabilities Manager Battle Command, "Trip Report," 10 – 25 June 2007.

(4) Weapons Technical Intelligence Handbook version 1.0, JIEDDO, September 2009.

(5) Ford, Thomas, C., Major, US Air Force, *Interoperability Measurement*, PhD Dissertation, Air Force Institute of Technology, August 2008.

(6) Chomsky, Noam, *Syntactic Structures*, (Mouton: The Hague/Paris, 1957).

(7) CIDNE terminology, Disconnected Automated Reporting Tool (DART) version 1.4.

(8) JOIIS terminology, Allied Command Transformation, NATO.

(9) PM Battle Command SIG-ACT Manager Overview and Requirements (document version 1.3).

(10) Tactics in Counterinsurgency, Army Field Manual 3-24.2, April 2009.

(11) DoD Net-Centric Data Strategy, May 9, 2003.

(12) Jones, S.G., "Counterinsurgency in Afghanistan," RAND Study Report, 2008.

(13) FBCB2 terminology, email communication from John Gillette, Deputy Program Manager, TIGR/THDD.

(14) CPOF terminology, email communication from Liz Roberts, Mowers Consulting, LLC.

(15) TIGR terminology, email communication from John Gillette, Deputy Program Manager, TIGR/THDD.

(16) Concept of Operations for Event/SIGACT Reporting, Version 3, Army TRADOC, US Army Combined Arms Center, Ft. Leavenworth, KS, June 24, 2009.

(17) DoD Command and Control Strategic Plan, OASD NII, January 12, 2009.

(18) American, British, Canadian, Australian and New Zealand Armies' Coalition Operations Handbook, November 2001.

Appendix D – Acronyms

ABCS	Army Battle Command System
BCT	Brigade Combat Team
BN	Battalion
C2	Command And Control
CIDNE	Combined Information Data Network Exchange system
C-IED	Counter Improvised Explosive Device
CO	Company
COIN	Counter Insurgency
CONOPS	Concept Of Operations
CPOF	Command Post Of the Future system
FBCB2	Force XXI Battle Command Brigade and Below system
DTG	Date-Time Group
GEOLOC	Geographical Location
IED	Improvised Explosive Device
JCIDS	Joint Capabilities Integration and Development system
JIEDDO	Joint Improvised Explosive Device Defeat Organization
JOIIS	Joint Operations/Intelligence Information System
JP	Joint Publication
MGRS	Military Grid Reference System
OCO	Overseas Contingency Operations
OSI	Open Systems Interconnect
PASS	Publish And Subscribe Service
POR	Program Of Record
SALUTE	Size, Activity, Location, Unit, Equipment
SIGACT	Significant Activity
TIGR	Tactical Ground Reporting System
TOC	Tactical Operation Center

TRADOC	US Army Training and Doctrine Command
TTPs	Tactics, Techniques, and Procedures
VBIED	Vehicle Borne Improvised Explosive Device
VMF	Variable Message Format
WTI	Weapons Technical Intelligence

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
May 2010	Study	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
US and Coalition Forces Data (Semantic) Interoperability Study	DASW01-04-C-0003
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Richard D. Bleach, Dale E. Lichtblau, Project Leader	
	5e. TASK NUMBER BC-5-3045
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	IDA Document D-4033

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Army CIO/G-6 National Center #3, Room 7136 2531 Jefferson Davis Highway Arlington, VA 22202	OASD(NII)CIO/G-6
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release, unlimited distribution: 24 May 2010.

13. SUPPLEMENTARY NOTES

IDA Document D-4018 is the unclassified/FOUO version of this document.

14. ABSTRACT

This research report documents the results of a study conducted in 2009 for the Army CIO/G-6 to assess the extent of data (or semantic) interoperability among certain US and coalition command and control (C2) information systems. The study focused on significant activity reports (SIGACTs) concerning counterinsurgency (COIN) and counter-improvised explosive device (C-IED) operations. An objective definition for semantic interoperability and a quantitative metric to measure it, based on shared or common reporting terminology, were developed and applied to four US and one coalition information systems. A major finding of the study was that today there is a low level of semantic interoperability between key US and coalition C2 information systems.

15. SUBJECT TERMS

Counterinsurgency (COIN), Significant Activity Reports (SIGACTS), Semantic, Data Interoperability

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Mr. Bruce Haberkamp
Unclassified	Unclassified	Unclassified	Unlimited	65	19b. TELEPHONE NUMBER (Include Area Code) (703) 607-7261